Local Arithmetic of Curves and Jacobians

Lectures by: Adam Morgan
Notes by: Ross Paterson

These notes were taken live during lectures at the CMI-HIMR Computational Number Theory summer school held at the University of Bristol in June 2019. In particular, any mistakes are the fault of the transcriber and not of the lecturer. Remarks in red were not written on the board, and were often added later by the transcriber.

Lecture List

Contents

Lecture 1: Introduction to Curves and Jacobians

Let K be a field

1 Some Words

An algebraic variety over K is a finite type separated K-scheme. By a curve we will mean an algebraic variety all of whose irreducible components have dimension 1. When we say "nice" about an algebraic variety we mean smooth, projective, geometrically integral. For nice algebraic varieties linear equivalence of divisors is the same as looking at line bundles.

2 Examples of Nice Curves

- The projective line: $\mathbb{P}^1_K = \mathrm{Proj}(K[X,Y])$, which over $\mathbb{C}$ is a Reimann sphere with genus 0.
- Elliptic curves: nice genus 1 curves with a specified K point. Over $\mathbb{C}$ these are tori and are isomorphic (as Lie groups) to $\mathbb{C}/\Lambda$ for a lattice Λ. If $\mathrm{char}(K) \neq 2, 3$ then these have a Weierstrass equation
$$E : y^2 = x^3 + ax + b$$
such that $\Delta_E = -16(4a^3 + 27b^2) \neq 0$. Note that this is affine and we really want the projective closure
$$y^2 z = x^3 + axz^2 + bz^3 \subset \mathbb{P}^2_K$$
which have one additional point at infinite, $[0 : 1 : 0]$ which is taken always to correspond to our fixed point O.
- Hyperelliptic curves: nice curve C of genus ≥ 2 with degree 2 (finite seperable) morphism $C \to \mathbb{P}^1_K$. We can always find a Weierstrass equation
$$C : y^2 = f(x)$$
with $f \in K[x]$ squarefree with $\deg(f) \in \{2g+1, 2g+2\}$ for g the genus of C, and such that
$$C \to \mathbb{P}^1_K$$
is the projection $(x, y) \mapsto x$. Note again that this is affine and we really mean the nice curve given by glueing the two affine charts
$$U_1 : y^2 = f(x)$$
$$U_2 : z^2 = w^{2g+2} f\left(\frac{1}{w}\right)$$

glued along $\{x \neq 0\}$ and $\{w \neq 0\}$ along the isomorphism $x = \frac{1}{w}$ and $y = \frac{z}{w^{g+1}}$. We call the points of $U_2 \backslash U_1$ the points at infinity, and note that this consists of 1 (resp 2) points if $\deg(f)$ is odd (resp. even).

Remark 2.1. *If $K = \overline{K}$, we've so far met all nice curves of genus $0, 1, 2$ and to cover genus 3 we also need smooth plane quartics*

$$f(x, y, z) = 0 \subset \mathbb{P}^1_K$$

for f degree 4 homomgeneous.

3 Abelian Varieties

3.1 Intro

E/K an elliptic curve with K rational point O. Then $E(K)$ has a natural group structure with identity O. One way to see this is the usual lines construction. Another way is to take the map

$$\begin{aligned} E(K) &\to \mathrm{Pic}^0(E/K) \\ P &\mapsto (P) - (O) \end{aligned}$$

which is a bijection by Reimann Roch and then we can pull back the group structure on $\mathrm{Pic}^0(E/K)$ to here. In fact these give the same group structure and this is a fun exercise.

Definition 3.1. *An* ***Abelian variety over*** *K is a nice group variety (i.e. a nice variety with a group structure given by morphisms).*

Remark 3.2. *This is certainly not the usual way to define abelian varieties, one usually starts with somewhat weaker hypotheses and actually shows that these varieties are nice. Further we have the following properties:*

- *The group structure on these is always abelian.*
- *1 dimensional abelian varieties are elliptic curves.*
- *Over $\mathbb{C}$ any abelian variety A is (as a complex Lie group) isomorphic to $\mathbb{C}^g/\Lambda$ for $g = \dim(A)$ and $\Lambda \subset \mathbb{C}^g$ a lattice.*

3.2 Torsion Points on Abelian Varieties

A/K an abelian variety of dimension g, then for any $n \geq 1$ coprime to $\mathrm{char}(K)$ we have

$$A[n] = A(\overline{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$$

in fact $A[n] \subseteq A(K^{\mathrm{sep}})$.

Definition 3.3 (Tate Module)**.** *let $\ell \nmid \mathrm{char}(K)$ be a prime then the ℓ-adic tate module is*

$$T_\ell(A) = \lim_{\leftarrow n} A[\ell^n]$$

We have a natural action of $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ on $A[\ell^n]$ making $T_\ell(A)$ into a G_K-module.

In fact, G_K acts $\mathbb{Q}_\ell$-linearly on $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, and we call this the **ℓ-adic Galois representation associated to** A.

4 Abelian Varieties over Number Fields

Let K be a number field, A/K an abelian variety.

Theorem 4.1 (Mordell-Weil)**.** *$A(K)$ is a finitely generated abelian group,*

$$A(K) \cong \mathbb{Z}^r \oplus \Delta$$

for Δ a finite abelian group. We call $r \geq 0$ the rank of the abelian variety and sometimes write $\mathrm{rk}(A/K)$.

Conjecturally, the rank is related to another important invariant of A/K, namely its L-function $L(A/K, s)$. For each non-archimedean place $v \in M_K$ write

$$I_v = \text{Inertia group at } v \qquad k_v = \text{Residue field at } v$$
$$\mathrm{Frob}_v = \text{(arithmetic) Frobenius at } v \qquad q_v = \# k_v$$

Definition 4.2. *For each v pick a prime $\ell \nmid v$. Define the local L-polynomial by*

$$L_v(A, T) = \det(1 - \mathrm{Frob}_v^{-1} T \mid (V_\ell(A)^*)^{I_v})$$

where $V_\ell(A)^*$ is the dual of $V_\ell(A)$.

It is a fact that $L_v(A, T) \in \mathbb{Z}[T]$ and is independent of our choice of ℓ. This follows from the Weil conjectures and the existence of the Neròn model.

Example 1. *E/K an elliptic curve, then*

$$L_v(E, T) = \begin{cases} 1 & E \text{ Additive at } v \\ 1 - T & E \text{ Split multiplicative at } v \\ 1 + T & E \text{ nonsplit multiplicative at } v \\ 1 - a_v T + q_v T^2 & E \text{ good at } v \end{cases}$$

where $a_v = q_v + 1 - \# E(k_v)$.

Definition 4.3. *The L-function of A/K is the complex function*

$$L(A/K, s) = \prod_{\substack{v \in M_K \\ non-arch}} L_v(A, q_v^{-s})^{-1}$$

This converges for $\mathrm{Re}(s) > \frac{3}{2}$ and conjecturally has analytic continuation to all of $\mathbb{C}$. There is much recent work in this direction, over $\mathbb{Q}$ we have Wiles work and some more recent things are being done for totally real number fields.

5 Jacobians

Let K be a field. Then

Definition 5.1 (/Theorem)**.** *Let C be a nice curve of genus g, then there exists some g dimensional abelian variety* $\mathrm{Jac}(C)$ *the* ***Jacobian*** *such that for any field extension L/K where $C(L) \neq \emptyset$ we have* $\mathrm{Jac}(C)(L) = \mathrm{Pic}^0(C/L)$ *functorially.*

In general even if $C(L) = \emptyset$ we have $\mathrm{Jac}(C)(L) = \mathrm{Pic}^0(C/K^{\mathrm{sep}})^{G_K}$.

Example 2. • *$\mathbb{P}^1_K$ has genus 0 so its Jacobain is 0 as is reflected in the isomorphism*

$$\mathrm{Pic}(\mathbb{P}^1_K) \xrightarrow{\deg} \mathbb{Z}$$

• *E/K an elliptic curve. Then E is its own Jacobian as is reflected in the isomorphism*

$$E(K) \to \mathrm{Pic}^0(E/K)$$

from earlier.

One thing we will do in this course is try to understand jacobians in terms of the underlying curve so that we can really write things down by hand.

6 Duality for Abelian Varieties

Definition 6.1 (/Theorem)**.** *Let A/K be an abelian variety, then there is another abelian variety $\check{A}/K$ called the dual of A with* $\dim(\check{A}) = \dim(A)$ *and such that for any L/K we have*

$$\check{A}(L) = \mathrm{Pic}^0(A/L)$$

(the line bundles which are algebraically equivalent to 0.)

In fact, $A, \check{A}$ are related by certain maps called **polarisations**. Let $\mathcal{L}$ be a line bundle on A, and $x \in A(K)$. Then consider

$$x \mapsto \tau_x^* \mathcal{L} \otimes \mathcal{L}^{-1} \in \mathrm{Pic}^0(A/K)$$

where τ_x is translation by x and in this way we get a homomorphism $\phi_{\mathcal{L}} : A \to \check{A}$.

Definition 6.2. *A **polarisation** is a homomorphism $\phi : A \to \check{A}$ such that over $\overline{K}$, $\phi = \phi_{\mathcal{L}}$ for some line bundle $\mathcal{L}$. A polarisation which is an isomorphism is called a **principle polarisation**.*

Proposition 6.3. *C/K a nice curve, with genus g. Let $J = \mathrm{Jac}(C)$. Then J is (canonically) principally polarised.*

Proof. First assume $C(K) \neq \emptyset$ then fix some $O \in C(K)$. For any n we have the **abel-jacobi** maps

$$\begin{aligned} C^n &\to \mathrm{Jac}(C) \\ (P_1, \dots, P_n) &\mapsto \left[\sum_{i=1}^n (P_i) - n(O)\right] \end{aligned}$$

For $n = g-1$, the image is a divisor on $\mathrm{Jac}(C)$ called the **Theta divisor** θ, and the polarisation ϕ is an isomorphism $J \to \check{J}$ independent of O. In general do this over the same extension of K. □

Lecture 2: Models of Curves

This will be the "theory of how to reduce things modulo primes".

7 Motivation: Elliptic Curves

Let p be a prime and say $p \neq 2, 3$, $E/\mathbb{Q}_p : y^2 = x^3 + ax + b$ for $a, b \in \mathbb{Q}_p$. After a change of variables $(x, y) \mapsto (u^2 x, u^3 y)$ for $u \in \mathbb{Q}_p^\times$ we may assume that $a, b \in \mathbb{Z}_p$ and that $\mathrm{ord}_p(\Delta_E)$ is minimal amongst all such equations. We call this a **minimal Weierstrass equation** for E. The reduction mod p is $\widetilde{E}/\mathbb{F}_p : y^2 = x^3 + \overline{a}x + \overline{b}$, which is well defined up to $\mathbb{F}_p$ isomorphism and we have 3 possible cases:

- $\widetilde{E}/\mathbb{F}_p$ an elliptic curve $\iff$ $\mathrm{ord}_p(\Delta_E) = 0$, we call this case **good reduction**.
- $\widetilde{E}/\mathbb{F}_p$ has a node $\iff$ $x^3 + \overline{a}x + \overline{b}$ has a root of multiplicity exactly 2, we call this case **multiplicative reduction**
- $\widetilde{E}/\mathbb{F}_p$ has a cusp $\iff$ $x^3 + \overline{a}x + \overline{b}$ has a root of multiplicity exactly 3, we call this case **additive reduction**

Remark 7.1. *In fact, we know things over extensions.*

- *If E has good/multiplicative reduction over $\mathbb{Q}_p$ then it also does over any finite extension $K/\mathbb{Q}_p$.*
- *If E has additive reduction then there is some finite extension $K/\mathbb{Q}_p$ over which E has either multiplicative or good reduction. Thus we sometimes refer to this as **semistable reduction***

In all cases, the set $\widetilde{E}_{ns}(\mathbb{F}_p)$ of nonsingular points has a natural group structure over $\mathbb{F}_p$.

8 Models of Curves

Let $K/\mathbb{Q}_p$ be a finite extension, and let $\mathcal{O}_K$ be the ring of integers, π_K a choice of uniformizer and k the residue field.

Definition 8.1. *A **model** of C is a scheme $\mathscr{C}/\mathcal{O}_K$ flat and proper over $\mathcal{O}_K$ and equipped with a specified isomorphism*

$$\mathscr{C} \times_{\mathcal{O}_K} K \to C$$

*where we call the left hand side the **generic fibre** of the model. We define the **special fibre** of the model to be the projective curve*

$$\mathscr{C}_k = \mathscr{C} \times_{\mathcal{O}_K} k$$

over k.

Example 3. *Let $E/\mathbb{Q}_p$ be an elliptic curve with minimal Weierstrass equation*

$$E : y^2 = x^3 + ax + b$$

$a, b \in \mathbb{Z}_p$. Then

$$\mathscr{E} : \left\{ y^2 z - x^3 - axz^2 - bz^3 = 0 \right\} \subset \mathbb{P}^2_{\mathbb{Z}_p}$$

is a model for E and has special fibre $\widetilde{E}/\mathbb{F}_p$.

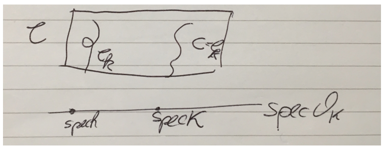

Figure 1: A model of a curve C

Want: An equation-free way of specifying the "best" model. Broadly there are 2 ways to go:

- Insist $\mathscr{C}/\mathcal{O}_K$ is regular. "Smooth as a surface", c.f. $y^2 = x^3 + x \subset \mathbb{A}^2$. This leads us to the **minimal regular model**
  - Can always find such a model,
  - Have intersection theory.

  but
  - Special fibre can be complicated,
  - Doesn't commute with ramified base change.
- Ask for special fibre to be as close to a nice curve as possible, maybe at the expense of replacing K by a finite extension. This leads us to the notion of **semistable/stable models**.

9 Structure of Singular Curves

Let k be a field, to start with we assume that $\overline{k} = k$. Let X/k be a projective, reduced, connected curve (note we are allowing singular points and multiple irreducible components). We denote by X_{sing} the (finite) set of singular points of X.

Definition 9.1. *The **normalisation** of X, $\widetilde{X}$ is the disjoint union of normalisations of the individual irreducible components. In particular $\widetilde{X}$ is a disjoint union of nice curves, and there is a canonical normalisation map*

$$\pi : \widetilde{X} \to X$$

which is an isomorphism away from the set of singular points.

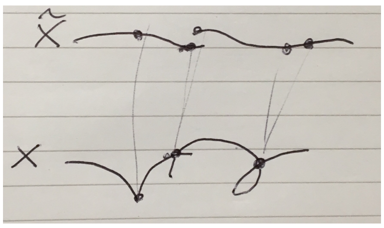

Figure 2: A visualisation of normalisation

Remark 9.2. *Locally over $U = \operatorname{spec} A \subset X$ the irreducible components meeting U are in bijection with minimal prime ideals of A say $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Then $\widetilde{U} := \pi^{-1}U$ is $\operatorname{spec} \prod_{i=1}^r \widetilde{A/\mathfrak{p}_i}$. And π is precisely the inclusion into the product, $\widetilde{A/\mathfrak{p}_i}$ is the integral closure of the domain $A/\mathfrak{p}_i$.*

We have a short exact sequence of sheaves on X

$$0 \longrightarrow \mathcal{O}_X \longrightarrow \pi_* \mathcal{O}_{\widetilde{X}} \longrightarrow S \longrightarrow 0$$

with S defined by the sequence, and S supported on X_{sing}.

Definition 9.3. *For $x \in X$ a closed point, define $\delta_x = \dim_k(S_x)$.*

- *Have $\delta_x = 0 \iff X$ smooth at x.*
- *Say x is an **ordinary double point** if $\delta_x = 1$ and $m_x := \left|\pi^{-1}\{x\}\right| = 2$.*

  Remark 9.4. *This is quite technical for a definition. It can be shown that x is an ordinary double point if and only if $\widehat{\mathcal{O}_{X,x}} \cong \frac{k[[u,v]]}{uv}$*

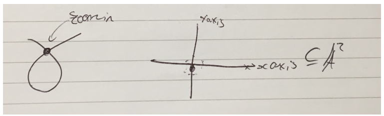

Figure 3: An ordinary double point.

- *Y an affine plane curve, $\{f(x,y) = 0\}$ with $(0,0) \in Y$. Then write $f(x,y) = \sum_i f_i$ as a sum of homogenous polynomials f_i of degree i. Then $(0,0)$ is smooth if and only if $f_1 \neq 0$, and is an ordinary double point if and only if $\operatorname{disc}(f_2) \neq 0$*

Definition 9.5. *We say that a (projective, reduced, connected) curve X is **semistable** if all the singular points are all ordinary double points. We say that X is stable if also $\operatorname{Aut}(X)$ is finite or equivalently X has arithmetic genus ≥ 2 and any irreducible component $\cong \mathbb{P}^1$ meets other components in ≥ 3 points.*

In general if $k \neq \overline{k}$ then say X is semistable/stable if $X_{\overline{k}}$ is (connected, reduced, projective and) semistable/stable.

10 the Dual Graph of a Semistable Curve

Definition 10.1. *$k = \overline{k}$ (else replace X with $X_{\overline{k}}$) then the **dual graph** of a semistable curve X is the graph $\mathcal{G}$ with vertices the irreducible components of X and edges the ordinary double points joining the components they lie on.*

Example 4. *1.*

$$y^2 = x^2(x-1)^2(x+1)^2 \tag{1}$$

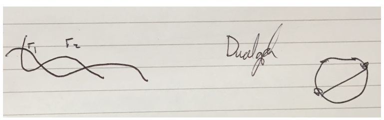

Figure 4: The dual graph of (1)

2.

$$y^2 = x^2(x-1)^2(x+1)^2(x-2) \tag{2}$$

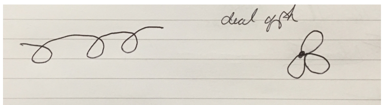

Figure 5: The dual graph of (2)

11 Semistable Models of Curves

Let $K/\mathbb{Q}_p$ be a finite extension, and C/K a nice curve.

Definition 11.1. *We say that C has **semistable reduction** if there exists a model $\mathscr{C}/\mathcal{O}_K$ for C with $\mathscr{C}_k$ a semistable curve over k. If there exists such a model where the special fibre is a nice curve then we say that C has **good reduction**. We call any model $\mathscr{C}/\mathcal{O}_K$ with (semi)stable special fibre a (semi)stable model.*

Theorem 11.2 (Deligne-Mumford)**.** *Let C/K be a nice curve, then there exists some L/K a finite extension such that C has semistable reduction over L.*

Moreover we have

Proposition 11.3. *If the genus of C is ≥ 2 and C has semistable reduction over L then it has a stable model $\mathscr{C}_{st}$ over L. This is unique up to $\mathcal{O}_L$-isomorphism and commutes with further extensions of L. We call its special fibre the **stable reduction** of C.*

Lecture 3: Clusters

Let us recall the notation thus far. Let $K/\mathbb{Q}_p$ be a finite extension with $\mathcal{O}_K, k, v_K$ the integers, residue field and normalised valuation. Let C/K be a nice curve of genus $g \geq 2$. Last time we had the Deligne-Mumford theorem which says that there is L/K finite such that C has a stable model $\mathscr{C}_{st}$ over L.

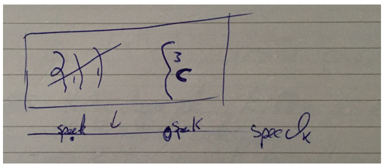

Figure 6: A model of a curve C.

12 Relationship between Stable Model and Minimal Regular Model

Suppose that C/K has semistable reduction, and $\mathscr{C}_{st}/\mathcal{O}_K$ is the associated stable model as in Theorem 11.2, Assume that each ordinary double point $x \in \mathscr{C}_{st,k}$ is **split** (i.e. both x and the two poinits over x in the normalisation of $\mathscr{C}_{st,k}$ are defined over k). Then for each ordinary double point x:

$$\widehat{\mathcal{O}_{\mathscr{C}_{st},x}} \cong \frac{\mathcal{O}_K[[u,v]]}{\langle uv - c\rangle}$$

for some $c \in \mathcal{O}_K$ with $v_K(c) \geq 1$. Call $n(x) = v_K(c)$ the **thickness** of x. We have that x is a regular point of $\mathscr{C}_{st}$ if and only if $n(x) = 1$. In general, the minimal regular model of C is obtained from $\mathscr{C}_{st}$ by replacing each ordinary double point x with a chain of $n(x)-1$ many copies of $\mathbb{P}^1$ meeting transversally (see Figure 7).

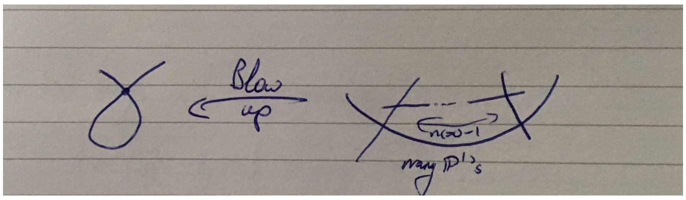

Figure 7: Obtaining the minimal regular model from the stable model.

Remark 12.1. *As the minimal regular model commutes with unramified extension and each ordinary double point is split over unramified extensions, we see that if C has semistable reduction then the regular model is semistable.*

13 Semistable Models of Hyperelliptic Curves

$K/\mathbb{Q}_p$ a finite extension with p odd, and fix C/K a hyperelliptic curve of genus ≥ 2.
Aim: Describe the stable model of C over a sufficiently large extension.
We do this by taking an example along the way

Example 5. *We take the genus 3 curve over $\mathbb{Q}_p$ (p odd):*

$$C : y^2 = x(x-p)(x-p^3)(x+p^3)(x-1)(x-1-p^2)(x-1+p^2)$$

We will compute:

- *$C/\mathbb{Q}_p$ has semistable reduction.*
- *Special fibre of the stable model is given in figure 11*

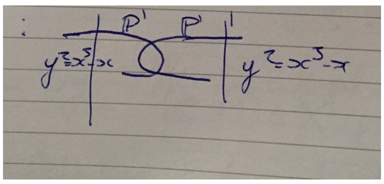

Figure 8: The special fibre of the stable model for Example 5

- *Minimal regular model is the stable model.*

Rough Idea: Have a degree 2 map $\phi : C \to \mathbb{P}^1$. Models of $\mathbb{P}^1$ can be described very explicitly – idea is to construct a model of C as a suitable double cover of a model of $\mathbb{P}^1$. By suitable we mean that the closure of the branch locus of ϕ has to have a particular shape.

Remark 13.1. *Bouw-Wewers study this more generally for cyclic covers of* $\mathbb{P}^1$ *and get an algorithm for computing stable models.*

Fix a Weierstrass equation for the hyperelliptic curve:

$$C : y^2 = f(x)$$

with $f \in K[x]$ of degree ≥ 5. Define

- c_f the leading coefficient of f
- $\mathcal{R}$ the set of roots of f in $\overline{K}$

Example 6 (5 continued)**.** *We have* $c_f = 1$, $\mathcal{R} = \{p, 0, p^3, -p^3, 1, 1+p^2, 1-p^2\}$

Assume:

1. $\mathcal{R} \subset K$ (else replace K by a finite extension)
2. $\deg(f) = 2g + 1$ (else change variables to move a point of the form $(r, 0)$ for $r \in \mathcal{R}$ to ∞)

Definition 13.2. *A* ***cluster*** *is a nonempty subset of* $\mathcal{R}$ *cut out by a disc. i.e. a nonempty subset* $S \subset \mathcal{R}$ *with* $S = \{r \in \mathcal{R} \mid v(r - z) \geq n\}$ *for some* $n \in \mathbb{Z}$ *and* $z \in K$ *(WLOG* $z \in \mathcal{R}$*).*

Call the maximal such n *the* ***depth*** *of* S*, denoted* d_S*.*

Example 7 (5 continued)**.** *The clusters of size at least 2 are:*

$$\begin{aligned}
\mathcal{R} &= \{p, 0, p^3, -p^3, 1, 1+p^2, 1-p^2\} & d_{\mathcal{R}} &= 0\\
S_1 &= \{1, 1+p^2, 1-p^2\} & d_{S_1} &= 2\\
S_2 &= \{p, 0, p^3, -p^3\} & d_{S_2} &= 1\\
S_3 &= \{0, p^3, -p^3\} & d_{S_3} &= 3
\end{aligned}$$

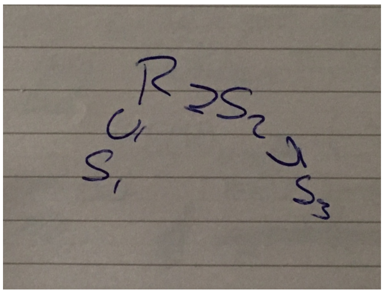

Figure 9: Inclusions for the clusters obtained from Example 5

Definition 13.3. *If* $S' \subset S$ *is a maximal proper subcluster then we call* S' *a* ***child*** *of* S *and* S *a* ***parent*** *of* S'*. We write* $S' \leq S$ *or* $S = P(S')$*.*

We say that S *is* ***odd/even*** *if* $|S|$ *is odd/even, and call* S ***übereven*** *if it is even and so too are all of its children.*

Definition 13.4. *Define the tree $\mathcal{T}_C$ with*

- *1 vertex v_S for each cluster S of size ≥ 3*
- *An edge between v_S and $v_{p(S)}$ for each $S \neq \mathcal{R}$.*
- *colour v_S yellow if S is übereven, blue otherwise.*
- *colour the edge between $S, p(S)$ blue if S is odd and yellow if S is even.*

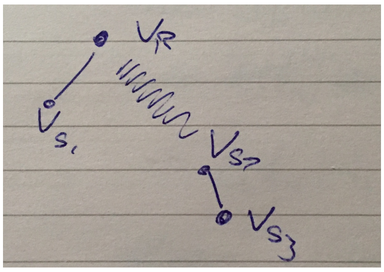

Figure 10: A sketch of the tree for Example 5

Example 8 (5 continued)**.**

13.1 The Stable Model of C

Assume for simplicity that there is no S of size $2g$. Then

1. C/K has semistable reduction if and only if for each cluster S of size ≥ 3

$$D_S := v_K(c_f) + |S|\, d_S + \sum_{r \notin S} v_K(z_S - r)$$

   is even (for any choice of $z_S \in S$).

2. If 1 holds then the dual graph of $\mathscr{C}_{st,\bar{k}}$ is the same as a graph $\mathcal{G}_C$ given by

   (a) Glueing 2 copies of $\mathcal{T}_C$ along the common blue part – call this $\widetilde{\mathcal{G}}_C$.

   (b) Add for each S with $|S| = 2$: a loop at the unique vertex of $\widetilde{\mathcal{G}}_C$ over $v_{p(S)}$ if $v_{p(S)}$ is blue; an edge between the 2 vertices of $\widetilde{\mathcal{G}}_C$ over $v_{p(S)}$ if $v_{p(S)}$ is yellow.

3. The normalisation of the component Γ_S corresponding to S of $\mathscr{C}_{st,\bar{k}}$ over a vertex v_S of $\mathcal{G}_C$ is the curve

$$\Gamma_S : y^2 = c_S \prod_{odd O \leq S} (x - \mathrm{red}_S(O))$$

   where $c_S \in K^\times$ is given by

$$c_S := \frac{c_f}{\pi^{v_K(c_f)}} \prod_{r \notin S} \frac{Z_S - r}{\pi^{v_K(Z_S - r)}} \mod \pi$$

   for Z_S any element of S and

$$\mathrm{red}_S(O) = \frac{Z_O - Z_S}{\pi^{d_S}} \mod \pi$$

   for Z_O any element of O.

13.2 The Minimal Regular Model of C

Let C be as above, assume that C/K is semisimple. The thickness of an ordinary double point x ($\leftrightarrow$ edge $e \in \mathcal{G}_C$ corresponding to $S \leq P(S)$) is

$$n(e) = \begin{cases} \frac{d_{p(S)}-d_S}{2} & e \text{ came from a blue edge} \\ d_{p(S)} - d_S & e \text{ came from a yellow edge} \\ 2d_{p(S)} - d_S & |S| = 2 \end{cases}$$

14 Néron Models of Abelian Varieties

As usual, $K/\mathbb{Q}_p$ finite and not we return to p arbitrary. For abelian varieties there exists an undisputed best model called the Néron model.

Definition 14.1 (/Theorem)**.** *Let A/K be an abelian variety. Then there exists a smooth, separated, finite type group scheme $\mathscr{A}/\mathcal{O}_K$ with generic fibre A and which satisfies the universal property (Néron mapping property):*

For any $\mathcal{Y}/\mathcal{O}_K$ smooth, any K-morphism $\mathcal{Y}_K \to A$ extends uniquely to an $\mathcal{O}_K$-morphism $\mathcal{Y} \to \mathscr{A}$.

This $\mathscr{A}$ is the Néron Model of A.

Remark 14.2. *We have traded properness for smoothness, but the Néron mapping property still forces $\mathscr{A}(\mathcal{O}_K) = A(K)$. In particular, we get a reduction map $A(K) \to \mathscr{A}_k(k)$ and we call $\mathscr{A}_k$ the reduction of A. This is a group variety over k.*

If $\mathscr{A}_k$ is an abelian variety then we say that A has good reduction, analogously to what we did for elliptic curves.

Definition 14.3. *Write $\mathscr{A}_k^\circ$ for the connected component of the identity in $\mathscr{A}_k$. We write $\mathscr{A}^\circ/\mathcal{O}_K$ for the open subscheme of $\mathscr{A}$ given by removing non identity cusps of the special fibre.*

We also write $A_\circ(K)$ for the points reducing to $\mathscr{A}^\circ(k)$, and the order of the group $A(K)/A_\circ(K)$ is the ***Tamagawa number*** *of A.*

Definition 14.4. *The* ***Tamagawa Number*** *is equivalently $\#(\mathscr{A}_k/\mathscr{A}_k^\circ)(k)$.*

Lecture 4: Tate Modules and local L-factors

We have the usual setup for this talk, Let $K/\mathbb{Q}_p$ be a finite extension with the usual data: $\mathcal{O}_K, k, v$.

14.1 Néron Models of Elliptic Curves

Proposition 14.5. *Let E/K be an elliptic curve, then we have:*

1. *The Néron model $\mathscr{E}/K$ of E is the smooth part of the minimal regular model of E.*
2. *The identity component $\mathscr{E}^\circ/\mathcal{O}_K$ is the smooth part of the minimal Weierstrass model of E (The $\mathcal{O}_K$-scheme defined by a minimal Weierstrass equation).*

I haven't mentioned the actual definition of minimal regular model, mainly because I forgot to actually concretely state it. A model $\mathscr{C}$ for a curve is **minimal** if for any other model $\mathscr{C}'$ the map on generic fibres corresponding to the identity on the curve extends to a morphism $\mathscr{C}' \to \mathscr{C}$. One can show that there always exists a regular model which is minimal in this sense, which we call the **minimal regular model**.

Example 9. *E/K with multiplicative reduction.*

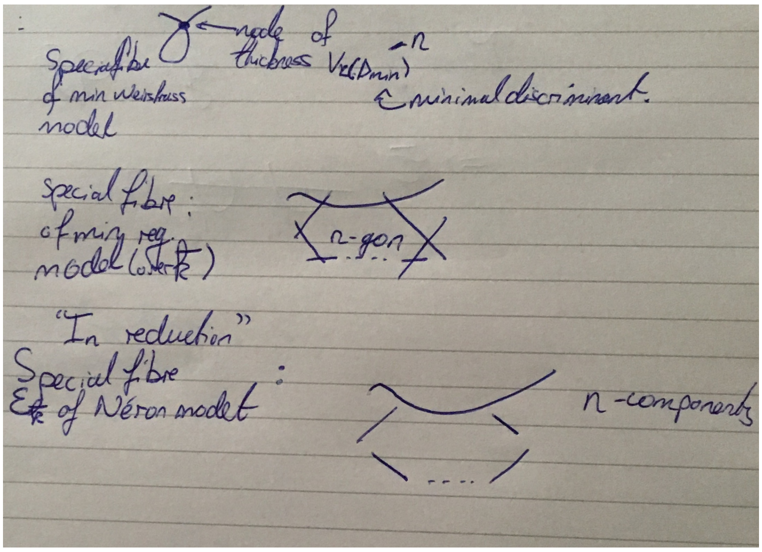

Figure 11: The special fibre of the stable model for Example 5

The component group is $\Phi = \frac{\mathscr{E}_k}{\mathscr{E}_k^\circ} \cong \mathbb{Z}/n\mathbb{Z}$ *with* Frob_k *acting as*

$$\begin{cases} 1 & \text{split mult reduction} \\ -1 & \text{split mult reduction} \end{cases}$$

Let C/K be a nice curve of genus g and $J = \mathrm{Jac}(C)$ which is a g dimensional abelian variety over K. Assume that $g \geq 2$ or C is an elliptic curve and let $\mathscr{J}/\mathcal{O}_K$ be the Néron model of J.

Theorem 14.6 (Raynaud)**.** *Let $\mathscr{C}/\mathcal{O}_K$ be one of*

- *A semistable model for C*
- *A regular model for C such that the* gcd *of multiplicities of the irreducible components of the special fibre is 1.*

Then the identity component of $\mathscr{J}/\mathcal{O}_K$ is $\mathrm{Pic}^0_{\mathscr{C}/\mathcal{O}_K}$ (the identity component of the relative picard functor – don't think too hard about what this means if you don't know!). In particular

- $\mathscr{J}_k^\circ = \mathrm{Pic}^0_{\mathscr{C}_k/k} \Rightarrow \mathscr{J}^\circ(\bar{k}) \cong \mathrm{Pic}^0(\mathscr{C}_{\bar{k}})$ *– the line bundles of degree 0 on $\mathscr{C}_{\bar{k}}$.*
- *If $\mathscr{C}$ has nice special fibre, i.e. C has good reduction, then $\mathscr{J}_k = \mathrm{Jac}(\mathscr{C}_k)$.*

Remark 14.7. *If $\mathscr{C}/\mathcal{O}_K$ is regular we can also describe the component group.*

14.2 The Tate Module of J

Assume that C/K is semistable, $\mathscr{C}/\mathcal{O}_K$ is any semistable model. Then J is also **semistable**, i.e. the identity component of its Néron models special fibre $\mathscr{J}_k^\circ$ is an extension of an abelian variety over k by a torus. In fact, the converse (J semistable gives C semistable) is also true.

Aim: To understand $T_\ell(J) = \lim_{\leftarrow_n} J[\ell^n] \circlearrowleft G_K$.

Remark 14.8. *As G_K-modules, $T_\ell(J)^\vee \cong H^1_{et}(C_{\overline{k}}, \mathbb{Z})$. We will explicitly describe $T_\ell(J)^{I_K}$, The unramified subgroup as a $\mathrm{Gal}(K^{\mathrm{nr}}/K) = G_k$ module. In fact,*

- *Action of the individual elements of I_K on $T_\ell(J)$ can be understood by the Grothendeick Picard-Lefschetz formula.*
  - *Can use this to construct transvections in the Galois image.*
- *If instead we only assume that C becomes semistable over some finite L/K then we can incorporate the $\mathrm{Gal}(L/K)$-action in the following to describe, for example, $T_\ell(J)^{I_K}$.*

Step 1: Since Néron models commute with unramified extensions (or using the Néron mapping property since $\operatorname{spec} \mathcal{O}_F \to \operatorname{spec} \mathcal{O}_K$ is smooth for F/K unramified).

We have a reduction map

$$J(K^{\mathrm{nr}}) \to J_k(\overline{k})$$

equivariant for the action of $G_k = \mathrm{Gal}(K^{\mathrm{nr}}/K) = \mathrm{Gal}(\overline{k}/k)$.

Proposition 14.9 (Serre-Tate)**.** *Reduction induces a G_k-module isomorphism*

$$T_\ell(J)^{I_K} \cong_{G_k} T_\ell(\mathscr{J}_k^\circ).$$

In particular, if J has good reduction, then $T_\ell(J)$ is unramified and

$$T_\ell(J) \cong_{G_K} T_\ell(\mathscr{J}_k)$$

with G_k action.

Adding in Raynauds theorem we now know

Corollary 14.10. *Whenever the conditions of Theorem 14.6 hold, we have that:*

$$T_\ell(J)^{I_K} \cong_{G_k} T_\ell(\mathrm{Pic}^0(\mathscr{C}_{\overline{k}}))$$

Remark 14.11. *If $\mathscr{C}$ has nice special fibre so that C has good reduction, we have*

$$T_\ell(J) \cong_{G_K} T_\ell(\mathrm{Jac}(\mathscr{C}_k))$$

as G_K-modules. Thanks to the Weil conjectures we can understand this (e.g. local factors of L-functions of J) by counting points on $\mathscr{C}_k$ over extensions of k.

Andrew Sutherland will go into detail on this next week.

Proposition 14.12. *Let $\mathcal{G}$ be the dual graph of $\mathscr{C}_{\overline{k}}$ and $\widetilde{\mathscr{C}_{\overline{k}}}$ the normalisation of $\mathscr{C}_{\overline{k}}$. Then we have a short exact sequence of G_k-modules*

$$0 \longrightarrow H^1(\mathcal{G}, \mathbb{Z}) \otimes \mathbb{Z}_\ell(1) \longrightarrow T_\ell(\mathrm{Pic}^0(\mathscr{C}_{\overline{k}})) \longrightarrow T_\ell(\widetilde{\mathscr{C}_{\overline{k}}}) \longrightarrow 0$$

where the first term is singular cohomology group of the graph $\mathcal{G}$ and $\mathbb{Z}_\ell(1) = \lim_{\leftarrow n} \mu_{\ell^n}$, the ℓ-adic tate module of $\overline{k}^\times$. Moreover

$$T_\ell(\mathrm{Pic}^0(\widetilde{\mathscr{C}_{\overline{k}}})) = \bigoplus_{\substack{G_k-\text{orbits of }\Gamma\\ \text{irred. component}\\ \text{of } \mathscr{C}_{\overline{k}}}} \mathrm{Ind}_{\mathrm{stab}\,\Gamma}^{G_K} T_\ell(\mathrm{Jac}(\widetilde{\Gamma}))$$

Remark 14.13. *G_K-action on $H^1(\mathcal{G},\mathbb{Z}) = \mathrm{Hom}(H_1(\mathcal{G},\mathbb{Z}),\mathbb{Z})$ is determined by the G_k-action:*

- *Components of $\mathscr{C}_{\overline{k}}$,*
- *Ordinary double points of $\mathscr{C}_{\overline{k}}$,*
- *Points of $\widetilde{\mathscr{C}_{\overline{k}}}$ lying over each ordinary double point thought of as edge endpoints.*

Sketch proof: Let $X = \mathscr{C}_{\overline{k}}$, $\widetilde{X} = \widetilde{\mathscr{C}_{\overline{k}}}$, $\pi : \widetilde{X} \to X$ the normalisation map and X_{sing} the ordinary double points of X. We have a short exact sequence

$$0 \longrightarrow \mathcal{O}_X^\times \longrightarrow \pi_*\mathcal{O}_{\widetilde{X}}^\times \longrightarrow \mathscr{F} \longrightarrow 0$$

for $\mathscr{F}$ some skyscraper sheaf supported on the singular points of X. Taking cohomology gives

$$0 \longrightarrow \mathcal{O}_X^\times(X) \longrightarrow \mathcal{O}_{\widetilde{X}}(\widetilde{X}^\times) \longrightarrow \mathscr{F}(X) \longrightarrow H^1(X,\mathcal{O}_X^\times) \longrightarrow H^1(X,\pi_*(\mathcal{O}_{\widetilde{X}}{}^\times)) \longrightarrow 0$$

where the first nonzero term is $\overline{k}^\times$, thes second is $\prod_{r \text{ irred cmpt}} \overline{k}^\times$, the third is $\prod_{x\in X_{\text{sing}}} \overline{k}^\times$, the fourth is $\mathrm{Pic}(X)$ and then the fifth the product $\prod_{\Gamma \text{irred cmpt}} \mathrm{Pic}(\widetilde{\Gamma})$, and the final term is 0 because $\mathscr{F}$ is flasque.

Restrict to degree 0 line bundles and get

$$0 \longrightarrow \overline{k}^\times \longrightarrow \prod_{\substack{\Gamma\\ \text{irred cpnt}}} \overline{k}^\times \longrightarrow \prod_{x\in X_{\text{sing}}} \overline{k}^\times \longrightarrow \mathrm{Pic}^0(\mathscr{C}_{\overline{k}}) \longrightarrow \prod_\Gamma \mathrm{Jac}(\widetilde{\Gamma})(\overline{k}) \longrightarrow 0$$

Take Tate modules and we find that

$$0 \longrightarrow \mathbb{Z}_\ell(1) \longrightarrow \bigoplus_\Gamma \mathbb{Z}_\ell(1) \longrightarrow \bigoplus_{x\in X_{\text{sing}}} \mathbb{Z}_\ell(1) \longrightarrow T_\ell(\mathrm{Pic}^0(\mathscr{C}_{\overline{K}})) \longrightarrow \bigoplus_\Gamma T_\ell(\mathrm{Jac}(\widetilde{\Gamma})) \longrightarrow 0 \tag{3}$$

On the other hand, with the simplicial chain complexes for $\mathcal{G}$ the 0-simplices (vertices) are irreducible components and the 1-simplices (edges) are ordinary double points so

$$0 \longrightarrow H_1(\mathcal{G},\mathbb{Z}) \longrightarrow \bigoplus_{edges} \mathbb{Z}\cdot e \longrightarrow \bigoplus_{vertices} \mathbb{Z}\cdot v \longrightarrow \mathbb{Z} \longrightarrow 0$$

Applying $\mathrm{Hom}(-,\mathbb{Z})\otimes\mathbb{Z}_\ell(1)$ and computing with (3) gives the result provided that we track the G_k action carefully. □

14.3 Computation of Local Factors of L-functions of J

Recall that the local L-polynomial is defined

$$L(J/K,T) = \det(1 - \mathrm{Frob}_K^{-1} T \mid (V_\ell(J)^\vee)^{I_K})$$

Corollary 14.14.

$$L(J/K,T) = \det\left(1 - \mathrm{Frob}_K^{-1}T \;\middle|\; H_1(\mathcal{G},\mathbb{Q}_\ell) \oplus \bigoplus_{\substack{G_k \text{ orbits} \\ \text{of irred cpnts } \Gamma}} \mathrm{Ind}_{\mathrm{stab}(\Gamma)}^{G_K} T_\ell(\mathrm{Jac}(\widetilde{\Gamma}))\right)$$

Proof. The Weil pairing on the tate module of J lands in $\mathbb{Z}_\ell(1)$ and gives $T_\ell(J)^\vee \cong T_\ell(J)(-1)$, called the Tate twist. In particular $(T_\ell(J)^\vee)^{I_K} \cong T_\ell(J)^{I_K}(-1)$. Then twist by (-1) in the proposition $\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$, and note that the characteristic polynomials depend only on the semisimplification of a representation and the first cohomology and homology are isomorphic representations. □

Example 10. *Let E/K be an elliptic curve with multiplicative reduction. Take the minimal Weierstrass model, so that the special fibre $\mathscr{C}_k$ is a nodal cubic curve. Then the Jacobian of the normalisation of the special fibre $\mathscr{C}_k$ is the Jacobian of $\mathbb{P}^1$ which is 0. Moreover $H_1(\mathcal{G},\mathbb{Q}_\ell)$ is isomorphic to $\mathbb{Q}_\ell$ with G_k acting trivially if E has split multiplicative reduction, and with* Frob *acting as multiplication by -1 in the case of non-split. Applying the Corollary above we obtain that*

$$L(E/K,T) = \begin{cases} 1-T & E \text{ has split multiplicative reduction} \\ 1+T & E \text{ has nonsplit multiplicative reduction} \end{cases}$$